IN THE CLAIMS:

Claims 6, 8-10, and 24-25 are amended. Claim 27 is canceled and claims 29 and 30 are added.

1-2. (Canceled)

3. (Previously Presented) The method of claim 6 wherein optimizing the decryption loop comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction.

4. (Original) The method of claim 3 wherein at least two of said techniques are combined synergistically.

5. (Canceled)

6. (Currently Amended) A computer-implemented method for determining whether computer code contains malicious code, said method comprising the steps of:

identifying computer code ~~suspected of currently containing malicious code, the computer code~~ having a decryption loop and a body;

performing a dead code elimination procedure on the computer code;

noting an amount of dead code eliminated during the dead code elimination procedure;

responsive to the amount of dead code eliminated during the dead code elimination procedure exceeding a preselected dead code threshold, declaring a suspicion of malicious code in the computer code;

optimizing the decryption loop to produce optimized loop code;

performing a malicious code detection procedure on the optimized loop code;

and

~~optimizing the body to produce optimized body code;~~

~~subjecting the optimized body code to a malicious code detection protocol;~~

~~and~~

responsive to the malicious code detection procedure detecting malicious code in the optimized loop code ~~or the malicious code detection protocol detecting malicious code in the optimized body code~~, declaring ~~a~~ confirmation that the computer code contains malicious code.

7. (Original) The method of claim 6 wherein the malicious code detection procedure is a procedure from the group of procedures consisting of pattern matching, emulation, checksumming, heuristics, tracing, and algorithmic scanning.

8. (Currently Amended) The method of claim [[6]] 29 wherein the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning.

9. (Currently Amended) The method of claim [[6]] 29 wherein the step of optimizing the body comprises using at least one output from the group of steps consisting of optimizing the decryption loop and performing a malicious code detection procedure on the optimized loop code.

10. (Currently Amended) The method of claim [[6]] 29 wherein, when the step of performing a malicious code detection procedure on the optimized loop code indicates the

presence of malicious code in the computer code, the steps of optimizing the body and subjecting the optimized body code to a malicious code detection protocol are aborted.

11. (Original) The method of claim 6 further comprising the additional step of, after the step of performing a malicious code detection procedure on the optimized loop code, revealing an encrypted body.

12. (Original) The method of claim 11 wherein the step of revealing an encrypted body comprises emulating the optimized loop code.

13. (Original) The method of claim 11 wherein the step of revealing an encrypted body comprises applying a key gleaned from the optimized loop code.

14. (Previously Presented) The method of claim 6, wherein optimizing the decryption loop to produce optimized loop code comprises:

performing a forward pass operation;

performing a backward pass operation;

performing a control flow graph reduction; and

iterating the above three steps a plurality of times.

15. (Original) The method of claim 14 wherein the iteration of the three steps stops after either:

a preselected number of iterations; or

observing that no optimizations of the computer code were performed in the most recent iteration.

16. (Original) The method of claim 14 further comprising the step of performing a code motion procedure, wherein the four steps are iterated a plurality of times.

17. (Previously Presented) The method of claim 14 wherein the forward pass operation comprises one or more steps from the set consisting of:

peephole optimization;

constant folding;

copy propagation;

forward computations related to abstract interpretation; and

instruction specialization.

18. (Previously Presented) The method of claim 14 wherein the backward pass operation comprises one or more steps from the set consisting of backward computations related to abstract interpretation and local dead code elimination.

19. (Original) The method of claim 18 wherein the backward pass operation comprises the additional step of global dead code elimination.

20-23. (Canceled)

24. (Currently Amended) A computer-readable storage medium containing executable computer program instructions for determining whether computer code contains malicious code, said computer program instructions performing the steps of:

identifying computer code ~~suspected of currently containing malicious code, the computer code~~ having a decryption loop and a body;

performing a dead code elimination procedure on the computer code;

noting an amount of dead code eliminated during the dead code elimination procedure;

responsive to the amount of dead code eliminated during the dead code elimination procedure exceeding a preselected dead code threshold, declaring a suspicion of malicious code in the computer code;

optimizing the decryption loop to produce optimized loop code;

performing a malicious code detection procedure on the optimized loop code; and

~~optimizing the body to produce optimized body code;~~

~~subjecting the optimized body code to a malicious code detection protocol; and~~

responsive to the malicious code detection procedure detecting malicious code in the optimized loop code ~~or the malicious code detection protocol detecting malicious code in the optimized body code~~, declaring ~~a confirmation~~ that the computer code contains malicious code.

25. (Currently Amended) The computer-readable medium of claim 24 wherein the malicious code detection ~~protocol~~ procedure is a ~~protocol~~ procedure from the group of ~~protocols~~ procedures consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning.

26. (Previously Presented) The computer-readable medium of claim 24 wherein optimizing the decryption loop comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction.

27. (Canceled)

28. (Previously Presented) The method of claim 6 wherein the malicious code detection procedure comprises emulating the optimized loop code.

29. (New) The method of claim 6, further comprising:

optimizing a body of the computer code to produce optimized body code;

subjecting the optimized body code to a malicious code detection protocol; and

responsive to the malicious code detection protocol detecting malicious code in the optimized body code, declaring that the computer code contains malicious code.

30. (New) The computer-readable medium of claim 24, wherein the computer program instructions are for further performing the steps of:

optimizing a body of the computer code to produce optimized body code;

subjecting the optimized body code to a malicious code detection protocol; and

responsive to the malicious code detection protocol detecting malicious code in the optimized body code, declaring that the computer code contains malicious code.